UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,658	03/28/2001	Pascal Paillier	032326-130	2508

21839 7590 09/22/2004

BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
POLTORAK, PIOTR	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/818,658	Applicant(s) PAILLIER, PASCAL	
	Examiner Peter Poltorak	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 June 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)☒ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

1. Claims 1-8 have been examined.

Priority

2. Foreign priority has been claimed in this application.

3. Acknowledgment is made of applicant's claim for foreign priority based on a French application filed on 3/28/2000. It is noted, however, that applicant has not filed a certified copy of the French application as required by 35 U.S.C. 119(b).

4. The effective priority date for the subject matter in the pending claims in this application once the paper has been received will be 3/28/2000.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-3 and 5-8 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

6. Claims 1-3, 5-6 fail to produce a "useful, concrete and tangible" result. The process does not produce a "useful, concrete and tangible" result; there is no clear output or an end point. Although method of generating electronic keys is discussed there is no indication of the keys produced and no entity benefiting of the keys is provided.

7. Claim 5 is rejected under 35 U.S.C. 101 because the claimed invention is not supported by either cryptographic keys generation asserted utility or a well

established utility. The step *A)* of claim 5 that suggests selecting *"b"* as a candidate key is not accurate *(See details in Claim Rejections).*

8. Claims 3, 7-8 are rejected by virtue of their dependence.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 4 and 5 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

10. The points A) and D) of claim 5 suggest that if $a^\wedge \lambda(b) \equiv 1(\mathrm{mod}\ b)$, "a" and "b" are public keys. However, in the art the letter "b" is used for creation of encryption and decryption keys and not the key itself *(Rudolf Lidl and Gunter Pilz, "Applied Abstract Algebra, pg. 289-290,the art uses letter "n" for "b").*

Applicant's preamble of the claim as well as the specification discloses method is used in context of RSA and RSA like cryptographic applications. In RSA applications "b" is not used as a key, but rather as a generator. Thus step A) of claim 5 that suggests selecting "b" as a candidate key, is not accurate.

11. Claim 4 is similarly rejected.

In order to give the claim further consideration the examiner will assume that the "said integers" cited in claim 4 are referring to integers which are verified to be co-primed, and that claim 5 is directed into verifying the co-primeness of numbers" a" and "b".

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 1-6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

13. "Said numbers" in claim 1 (line 2) lacks antecedent basis.

14. It is not clear whether claims 1, 5 and 6 are simply incomplete omitting essential steps or whether the claims are directed only towards verification of the co-primeness of said numbers "a" and "b" in context of generating cryptographic keys. The claims are directed to a method generating electronic keys; however, the claims only provide methods of verifying the co-primeness of said numbers "a" and "b" and not steps of producing the electronic key being offered.

15. In order to give the claim further consideration the examiner will assume that the claims 1, 5-6 are directed to verifying the co-primeness of numbers" a" and "b".

16. Claims 2-4 are rejected by virtue of their dependence.

Appropriate correction is required

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. **Claim 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rudolf Lidl and Gunter Pilz *("Applied Abstract Algebra", ISBN 0387961666, 1985; hereinafter Lindl et al.)*, and further in view of the admitted prior art (AAPA) and Bruce Schneier *("Applied Cryptography, protocols, algorithms, and source code in C",ISBN: 0471128457, 1996)*.**

18. *Lindl et al.* teach a method of generating keys RSA. *Lindl et al.* teach that φ(n) may be replaced in the Euler theorem by the Carmichael function λ(b) *(Lindl et al., pg. 290, letter "n" is used instead of "b")* so

$$a\wedge \lambda(b) \equiv 1(mod\ b)$$

19. *Lindl et al.* do not teach a step of verifying the co-primeness of said numbers a, b, and storing a number "a" in memory.

20. The admitted prior art teaches an algorithm verifying the co-primeness of two numbers by selecting an integer number "a" drawn at random, choosing and storing in memory an integer number "b", and verifying the co-primeness between numbers "a" and "b" *(Background of the Invention, pg.1 and 2).*

21. The motivation to combine is suggested by *Schneier* who discloses the advantages of applying a co-primeness verification such as that of AAPA to a number generation method such as that of *Lidl et al's (Schneier , last§ on pg. 258).*

22. The limitation of reiterating verification operations with another pair of numbers when equality is not verified (the modular expansion is not equal to 1), and retaining the pair when equality is verified, is implicit in the method of generation cryptographic keys.

23. The limitations of claim 3 are implicit in the $a^\wedge \lambda(b) \equiv 1(mod\ b)$ equation. In order to verify the equation the number "b" must be predetermined *(selected prior to the equation verification)* the value of $\lambda(b)$ must be calculated in advance and stored in a memory before any other operation on the equation could be done.

24. As per claim 4 *Lindl et al.* and *AAPA* teach verifying the co-primeness of numbers as discussed above.

25. *Lindl et al.* and *AAPA* do not teach encrypting and/or decrypting information by means of a public key cryptography protocol, using said integers as the encryption and decryption keys.

26. The motivation to encrypt and/or decrypt information by means of a public key cryptography protocol, using verified co-primary integers as the encryption and decryption keys is suggested by Schneier which teaches that public-key algorithms need prime numbers *(pg. 258 § 2)* and discloses benefits of communications using public-key cryptography *(pg. 31-32).*

27. **Claim 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rudolf Lidl and Gunter Pilz *("Applied Abstract Algebra", ISBN 0387961666, 1985; hereinafter Lindl et al.)* in view of the admitted prior art (AAPA), Bruce Schneier *("Applied Cryptography, protocols, algorithms, and source code in C",ISBN: 0471128457, 1996)* and further in view of Murphy et al. *(U.S. Patent No. 6226744).***

28. The operations verifying the co-primeness of integer numbers which that are part of a method for generating electronic keys have been addressed as cited in claim 6 and are substantially equivalent to the limitations of claim 1 as taught by *Schneier, Lidl et al.* and *AAPA*; therefore the limitations of claim 6 referring to the operations are similarly rejected.

29. *Schneier, Lidl et al.* and *AAPA* do not teach the operations implemented on a portable electronic device comprising an arithmetic processor and an associated program memory that are capable of effecting modular exponentations.

30. *Murphy et al.* teach a portable electronic device including a chip card with an arithmetic microprocessor and an associated program memory that are capable of effecting modular exponentiations, and which generates electronic keys including RSA *(Murphy et al., col. 5 lines 60-65 and col. 2 lines 44-64).*

31. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use the portable electronic device to implement verifying the co-primeness. One of ordinary skill in the art would have been motivated to perform

such a modification in order to make the operations easier and more efficient to perform.

32. The limitations of claim 7 are implicit in the *a^ λ(b) ≡1(mod b)* equation. In order to verify the equation the number "b" must be predetermined *(selected prior to the equation verification)* the value of *λ(b)* must be calculated in advance and stored in a memory before any other operation on the equation could be done.

Conclusion

No claim is allowed.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (703) 305-0719. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Signature

8/23/04

Date

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100